

REMARKS

This Amendment is submitted in response to the Office Action dated March 22, 2006, having a shortened statutory period set to expire June 22, 2006. Proposed amendments to the Claims include **amending** Claims 1-2 and **adding** Claims 3-4. Upon entry of the proposed amendments, Claims 1-4 will now be pending.

Applicants appreciate the time and courtesy extended by Examiner Stoyrnor and Supervisor Browne during a June 21, 2006 teleconference. An agreement was reached that Claim 2, as presently amended, is not taught or suggested by the cited prior art. If Applicants' undersigned representative has misunderstood this agreement, telephonic notification at the Examiner's earliest convenience would be greatly appreciated.

Double Patent Rejection

On Page 2 of the present Office Action, the Examiner has presented a non-statutory obviousness-type double patenting rejection against co-pending U.S. Patent Application Nos. 10/674,776, 10/675,624 and 10/698,128. Appropriate terminal disclaimers are enclosed herein, and thus this rejection should be withdrawn.

Claim objections

On Page 4 of the present Office Action, Claim 1 is objected to for the typographical error of "compute" instead of "computer" at line 7. Applicants appreciate the Examiner's close inspection of the claim, and correct the noted error in the present amendment. This objection should thus be withdrawn.

Rejection under 35 U.S.C. § 103

On Page 4 of the present Office Action, Claims 1-2 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Zimmer et al.* (U.S. Patent Application Publication No. 2004/0193867 – “*Zimmer*”) in view of *Schell et al.* (U.S. Patent No. 6,314,520). Applicants respectfully traverse these rejections.

With regards to **Claim 1**, the cited art does not teach or suggest “under the control of a remote supervisory computer connected via a hyper-secure link to a client computer, storing a list of trusted configuration servers in a Remote Supervisor Adapter (RSA) card on the client computer”, as supported in the present specification at paragraph [0016]. While the cited art references a Network Interface Card (NIC), the combination of the cited prior art does not teach or suggest the use of an RSA card. Claim 4, which is supported by paragraph [0016] of the present application, is added to clarify the feature that the remote supervisory computer is performing the storing of the list of trusted configuration servers in an RSA card on the client computer.

*Zimmer* is cited for teaching that a server can be securely connected to a client to download boot images (*Zimmer* Figures 1 and 4). Examiner notes that *Zimmer* fails to disclose storing a list of trusted configuration servers in the client computer. However, at col. 2, lines 30-35, col. 3, lines 6-11, col. 4 line 64 to col. 5, line 2, and col. 5, lines 13-22, *Schell* teaches that a NIC can store addresses of trusted servers, which are compared to the source address of incoming packets.

The Examiner’s position, as understood by the Office Action and the June 21, 2006 teleconference, is essentially that *Zimmer* teaches that a server can control a client, *Schell* teaches that a client computer can store a list of trusted servers in the client computer’s NIC, so therefore the combination teaches that a secure server can store the list of trusted computers in the client computer.

Consider now *Schell* at col. 6, lines 8-20:

“Initialization continues with step 124 wherein the CPU executes the program instructions resident in the NIC BIOS 65 (FIG. 3) to initialize the hardware in the NIC. Following hardware initialization, the CPU downloads the pre-boot modules from the server in step 126 and in step 128, executes these pre-boot modules to perform the identification and authorization function associated with the login process described in FIG. 6. In addition the CPU loads the registers of the NIC's send address confirmation circuitry 66 and the receive address confirmation circuit 88 (FIG. 3) with values stored in the NIC BIOS ROM. In an alternative embodiment, the pre-boot modules may be stored in the NIC BIOS.”  
(emphasis added)

As stated in Section 2143.03 of the MPEP, it is axiomatic that the prior must teach or suggest every claim limitation. Neither *Schell* nor *Zimmer* teaches a supervisory computer storing a list of trusted configuration servers in the client computer. The combination of *Zimmer* (a supervisory computer) with *Schell* (a client computer loading the list in a NIC) does not teach or suggest the limitation of the supervisory computer storing the list in the client. That is, the combination of the cited art teaches that the information as to which server is to be trusted comes NOT from a remote supervisory computer, but from the client computer itself (i.e., from the client computer's NIC BIOS). There is no suggestion that the storage of such a list may come from, and be under the control of, a remote supervisory computer. The fact that a server can control a client does not teach or suggest the scenario in which the remote supervisory computer performs the storing of the list of trusted configuration servers in the client computer.

With regards now to **Claim 2**, the combination of the cited art does not teach or suggest “in response to determining that the responding configuration server is not on a list of trusted configuration servers, selecting, by the client computer, a selected server from one of the servers on the list of trusted configuration servers; and requesting the configuration parameters from the selected server,” as supported in the present specification by Figure 3, blocks 318 and 308.

*Schell* is cited for teaching the discarding of packets that are from untrusted locations, and accepting only packets from trusted locations. There is no teaching or suggestion of getting a configuration parameter from a server that is selected from the list of trusted configuration servers. That is, *Schell* examines the source address of incoming packets, while Claim 2 relates to the client computer choosing a server to make a call to.

Regarding new Claim 3, the cited art does not teach or suggest "wherein the remote supervisory computer is a Pre-boot eXecution Environment (PXE) deployment server that is managed by an Information Technology (IT) services organization that manages various types of PXE deployment servers, and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer," as supported in paragraph [0021] of co-pending U.S. Patent Application No. 10/674,776 (which has been incorporated by reference by the present application).

CONCLUSION

For the reasons stated above, Applicants now respectfully request a Notice of Allowance for all pending claims.

Applicant further respectfully requests the Examiner contact the undersigned attorney of record at 512.617.5533 if such would further or expedite the prosecution of the present Application.

No extension of time for this response is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application, including any required fees associated with the included Terminal Disclaimers, to **IBM CORPORATION DEPOSIT ACCOUNT No. 50-0563**.

Respectfully submitted,



James E. Boice  
Registration No. 44,545  
DILLON & YUDELL LLP  
8911 North Capital of Texas Highway  
Suite 2110  
Austin, Texas 78759  
512.343.6116

ATTORNEY FOR APPLICANT(S)